CLAIMS

1. A method of delegating key-provision authority to a device from a trusted authority, the method comprising providing a yet-to-be completed chain of public/private cryptographic key pairs linked in a subversion-resistant manner and comprising:

a starting key pair formed by a public/private key pair of the trusted authority,

a penultimate key pair formed by public/private data, the private data being securely stored in the device for access only under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion–resistant operating environment, and

a link between the penultimate key pair and an end key pair to be formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme; this link being said key-generation process arranged to execute in said subversion–resistant operating environment on the device to generate said decryption key using said private data and the IBE encryption key and to make the generated key available for use.

2. A method according to claim 1, wherein said key-generation process is arranged to check that at least one condition has been satisfied before the process generates the decryption key and/or makes the key available for use.

3. A method according to claim 2, wherein said at least one condition comprises a condition to be presented to the device in said encryption key.

4. A method according to claim 3, wherein said condition indicated in said encryption key is a condition that is to be met by particular data stored in the device, this data having been provided by the trusted authority and stored in the device protected against subversion.

5. A method according to claim 3, wherein said condition indicated in said encryption key is a condition that is to be satisfied by input data presented by a user of the device.

6. A method according to claim 2, wherein said at least one condition comprises a condition to be presented in encrypted form to the device.

7. A method according to claim 2, wherein said at least one condition comprises a condition that input data presented by a user of the device has a predetermined relationship with particular data stored in the device and protected against subversion.

8. A method according to claim 7, wherein said at least one condition is a user authentication condition concerning a current user of the device.

9. A method according to claim 1, wherein said penultimate key pair is the second key pair in said chain, the start key pair and penultimate key pair being linked by said public data being certified by the trusted authority, using its private key, to indicate that an entity holding the corresponding said private data is one to which it has delegated authority.

10. A method according to claim 1, wherein said penultimate key pair is the third key pair in said chain, the private key of the second key pair being securely stored in the device, and the start key pair and the second key pair being linked by the public key of the second key pair being certified by the trusted authority, using its private key, to indicate that an entity holding the private key of the second key pair is one to which it has delegated authority; the second key pair being linked to the penultimate key pair by said key-generation process being arranged to be activated in order to respond to a challenge based on the public key of the second key pair before attempting to complete said chain by providing said decryption key.

11. A method according to claim 1, wherein the private key of at least one key pair of said chain, additional to the first key pair, is held outside said device.

12. A method according to claim 1, wherein the or each link in at least the portion of the chain extending from the starting key pair to the penultimate key pair is verifiable by a party wishing to rely on the delegation of authority to the device from the trusted authority.

13. A method according to claim 12, wherein at least one of the verifiable links is verifiable as a result of the public key of the downstream key pair associated with the link being certified using the private key of the upstream key pair associated with that link.

14. A method according to claim 1, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment.

15. A method according to claim 14, wherein the trusted authority checks the trusted platform status of the device.

16. A method according to claim 14, wherein said public data is held in protected storage and only accessible by the key-generation process when executing in said subversion-resistant operating environment.

17. A method according to claim 4, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment, said public data and said particular data being held in protected storage and only accessible by the key-generation process when executing in said subversion-resistant operating environment.

18. A method according to claim 17, wherein said particular data is profile data for a party associated with the device.

19. A data access control method involving delegated authority, the method comprising:

- attempting to complete a chain of public/private cryptographic key pairs linked in a subversion-resistant manner and comprising:
  - a starting key pair formed by a public/private key pair of a trusted authority,
  - a penultimate key pair formed by public/private data, the private data being securely stored in a device for access under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion–resistant operating environment, and

- a link between the penultimate key pair and an end key pair to be formed by an encryption/decryption key pair of an Identifier-Based Cryptographic, IBE, scheme; this link being said key-generation process arranged to execute in said subversion–resistant operating environment on the device to provide the IBE decryption key, generated using said private data and the IBE encryption key,

attempted completion of said chain being effected by executing said key-generation process in said subversion–resistant operating environment on the device; and

- where execution of the key-generation process results in the provision of the decryption key, using the decryption key to decrypt data encrypted using said public data and said IBE encryption key.

20. A method according to claim 19, wherein said key-generation process checks that at least one condition has been satisfied before the process generates the decryption key and/or makes the key available for use.

21. A method according to claim 20, wherein said at least one condition comprises a condition presented to the device in the IBE encryption key.

22. A method according to claim 21, wherein said condition indicated in said encryption key is a condition that is checked by reference to particular data stored in the device, this data having been provided by the trusted authority and stored in the device protected against subversion.

23. A method according to claim 21, wherein said condition indicated in said encryption key is a condition that is checked by reference to input data presented by a user of the device.

24. A method according to 21, wherein said at least one condition comprises a condition that is checked by comparing input data presented by a user of the device with particular data stored in the device, this data having been provided by the trusted authority and stored in the device protected against subversion.

25. A method according to claim 20, wherein said at least one condition comprises a condition presented in encrypted form to the device.

26. A method according to claim 19, wherein said penultimate key pair is the second key pair in said chain, the start key pair and penultimate key pair being linked by said public data being certified by the trusted authority, using its private key, to indicate that an entity holding the said private data is one to which it has delegated authority.

27. A method according to claim 19, wherein said penultimate key pair is the third key pair in said chain, the private key of the second key pair being securely stored in the device, and the start key pair and the second key pair being linked by the public key of the second key pair being certified by the trusted authority, using its private key, to indicate that an entity holding the private key of the second key pair is one to which it has delegated authority; the second key pair being linked to the penultimate key pair by said key-generation process being activated in order to respond to a challenge based on the public key of the second key pair before attempting to complete said chain by providing said decryption key.

28. A method according to claim 19, wherein the private key of at least one key pair of said chain, additional to the first key pair, is held outside said device.

29. A method according to claim 19, wherein the or each link in at least the portion of the chain extending from the starting key pair to the penultimate key pair is verified by a party wishing to rely on the delegation of authority to the device from the trusted authority.

30. A method according to claim 29, wherein at least one of the verified links is verified on the basis of a certificate for the public key of the downstream key pair associated with the link, this certificate being a certificate certified using the private key of the upstream key pair associated with that link.

31. A method according to claim 19, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment.

32. A method according to claim 31, wherein said public data is held in protected storage and only accessible by the key-generation process when executing in said subversion-resistant operating environment.

33. A method according to claim 19, wherein the encrypted data is data encrypted by a service provider, decryption of the encrypted data being required in order to gain access to a service provided by the service provider.

34. A method according to claim 33, wherein the encrypted data provided by the service provider is a data component of the service.

35. A method according to claim 33, wherein the encrypted data provided by the service provider is arbitrary data, the method further comprising returning the decrypted data to the service provider as evidence that said conditions have been met, and the service provider thereafter providing said service to the party.

36. A method according to claim 33, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment, the service provider checking the trusted platform status of the device before providing said service.

37. A method of delegating authority to a device from a trusted authority, the method comprising:

securely storing in the device a private data item for access only under circumstances that has been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion–resistant operating environment;

providing a public data item associated with said private data item and certified by the trusted authority to indicate that an entity holding the private data item is one to which it has delegated authority;

arranging for said key-generation process to execute in said subversion–resistant operating environment on the device to generate a decryption key using said private data item and a third-party-supplied encryption key.

38. A method according to claim 37, wherein key-generation process only generates the decryption key , or only makes it available for use, if at least one condition, indicated in the encryption key, has been satisfied.

39. A method according to claim 38, wherein said condition indicated in said encryption key is a condition that is to be met by particular data stored in the device, this data having been provided by the trusted authority and stored in the device protected against subversion.

40. A method according to claim 38, wherein said condition indicated in the encryption key is a condition that is to be satisfied by input data presented by a user of the device.

41. A method according to claim 38, wherein said condition indicated in the encryption key is a condition that input data presented by a user of the device has a predetermined relationship with particular data stored in the device and protected against subversion.

42. A method according to claim 38, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment.

43. A method according to claim 38, wherein the public data item is held in protected storage and only accessible by the key-generation process when executing in said subversion-resistant operating environment.

44. A method of controlling access to a service provided by a service provider, the method comprising:

- the service provider providing encrypted data to a device which is associated with a party wishing to receive said service and which securely stores a private data item, the service provider generating said encrypted data by encrypting data using an encryption key and a public data item certified by a trusted authority as associated with said private data item, decryption of the encrypted data being required in order to receive said service;
- executing at the device a key-generation process that only has access to the private data item if the process and the operating environment in which it runs have been pre-authorised by the trusted authority, the key-generation process itself only providing a decryption key, generated using said private data item and said encryption key, if at least one condition is satisfied, said at least one condition comprising a condition indicated in the encryption key;
- using the decryption key to decrypt said encrypted data.

45. A method according to claim 44, wherein said condition indicated in said encryption key is a condition that is checked by reference to particular data stored in the device, this data having been provided by the trusted authority and stored in the device protected against subversion.

46. A method according to claim 44, wherein said condition indicated in the encryption key is a condition that is checked by reference to input data presented by a user of the device.

47. A method according to claim 44, wherein said condition indicated in the encryption key is a condition that is checked by comparing input data presented by a user of the device with particular data stored in the device and protected against subversion.

48. A method according to claim 44, wherein the data that is encrypted by the service provider is a data component of the service.

49. A method according to claim 44, wherein the data that is encrypted by the service provider is arbitrary data, said party returning the decrypted data to the service provider as evidence that said at least one condition has been met, and the service provider thereafter providing said service to the party.

50. A method according to claim 44, wherein the device comprises a trusted platform arranged to execute the key-generation process in the operating environment pre-authorised by the trusted authority.

51. A method according to claim 50, wherein the service provider checks the trusted platform status of the device before providing said service.

52. A method according to claim 50, wherein the public data item are held in protected storage and only accessible by the key-generation process when executing in the operating environment pre-authorised by the trusted authority.

53. A system comprising:

- a trusted authority entity including secure storage means for securely storing a private key of a first public/private key pair, and
- a device arranged to serve as a delegate for said trusted authority, the device including secure storage means;

the system being arranged to host at least the private keys of a chain of public/private cryptographic key pairs that are linked in a subversion-resistant manner, this chain comprising:

- a starting key pair formed by said first key pair,
- a penultimate key pair formed by public/private data; and
- an end key pair formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme;

the secure storage means of the device being arranged to securely store said private data for access only by authorised means pre-authorised by the trusted authority, the device further including said authorised means for linking said penultimate and end key pairs, said authorised means being arranged to provide said decryption key, generated using said

private data and said IBE encryption key, only if at least one condition is satisfied, said at least one condition comprising a condition indicated in the encryption key.

54. A system according to claim 53, wherein said condition indicated in said encryption key is a condition that is to be met by particular data stored in the device and protected against subversion, the said authorised means being arranged to check this condition by reference to said particular data.

55. A system according to claim 53, wherein said condition indicated in the encryption key is a condition that is to be satisfied by input data presented by a user of the device, the device including input means for receiving said input data and the said authorised means being arranged to check the condition indicated in the encryption key by reference to said input data.

56. A system according to claim 54, wherein said condition indicated in the encryption key is a condition that input data presented by a user of the device has a predetermined relationship with particular data stored in the device and protected against subversion, the device including input means for receiving said input data and the said authorised means being arranged to check the condition indicated in the encryption key by comparing said input data with said particular data.

57. A system according to claim 53, in which the private key of the first key pair is securely stored in the storage means of the trusted authority entity, and said private data is securely stored in the storage means of the device.

58. A system according to claim 53, wherein said penultimate key pair is the second key pair in said chain, the trusted authority entity being arranged to provide the link between the start key pair and penultimate key pair by using the private key of the first key pair to certify said public data such as to indicate that an entity holding the corresponding private data is one to which it has delegated authority.

59. A system according to claim 53, wherein said authorised means is a key-generation process and a subversion-resistant operating environment for running said key-generation process.

60. A device arranged to serve as a delegate for a trusted authority, the device comprising:

a trusted computing platform for providing a subversion-resistant operating environment for running processes, the trusted computing platform including secure storage means securely storing private data provided by the trusted authority, the secure storage means being arranged to provide access to the private data only in circumstances pre-authorised by the trusted authority and involving a specific key-generation process running in said subversion-resistant operating environment; and

a program memory storing program code corresponding to said key-generation process, said process when run serving to generate an Identifier Based Encryption decryption key using a third-party-supplied encryption key string and said private data, the process being arranged only to generate the decryption key, or only to make it available for use, if at least one condition, indicated in said encryption key string, has been satisfied.